

1 PASSWORD GENERATION AND VERIFICATION SYSTEM
2 AND METHOD THEREFOR
3

4 CROSS-REFERENCE TO RELATED APPLICATION
5

6 This application claims priority to Japanese Patent
7 Application No. 2000-391720, filed 25 December 2000.
8

9 Field of the Invention
10

11 The present invention relates to systems and methods for
12 verifying a password, and more specifically to a system and
13 method for selecting and verifying elements that comprise a
14 password on an element-by-element basis.
15

16 Background of the Invention
17

18 For access to computer systems and specific programs,
19 activation of electronic devices, unlocking of doors, and so
20 forth, a password is used to ensure security, so that only an
21 owner of such security authorization can access the computer
22 system, for example. The password typically comprises a
23 combination of multiple alphabets and numerals. The user of
24 the computer system registers his predetermined password with

1 the system and enters that password whenever he accesses the
2 system. The system compares the entered password against the
3 registered password, and, if they match, grants him access to
4 the system.

5
6 In order to prevent unauthorized access effectively, a
7 password should preferably be alphanumeric characters
8 consisting of a complex combination of alphabets and
9 numerals. However, because it is difficult to accurately
10 remember complicated alphanumeric characters for a long
11 period of time, a password comprising a easy-to-remember
12 combination of alphanumeric characters, for example, a
13 password including the name and/or birth date of the user, is
14 chosen. Such a password is readily deciphered by an
15 unauthorized intruder so that it is easily allowed to gain
16 access to the system.

17
18 In order to overcome such shortcomings, it is
19 recommended not to use passwords that contain meaningful
20 words, including, for example, common nouns, people's names,
21 geographical names, and country names; additionally, security
22 for passwords is enhanced by, for example, periodically
23 changing the password. Such solutions inevitably result in
24 reduced usability of passwords, so that an easy-to-remember

1 password is eventually preferred. In other words, when
2 security for a password is enhanced, its usability is
3 degraded, whereas when its usability is improved, its
4 security is lowered.

5

6 Furthermore, as social life diversifies into various
7 activities, the opportunity for using passwords will
8 increase. Passwords are demanded in many cases, for example,
9 when a bank account is accessed from the ATM (Automatic
10 Teller Machine), when the computer is started up, and when an
11 online transaction is performed over the Internet. It is
12 quite difficult to remember and manage a plurality of those
13 passwords. As a result, there may be scenarios where you may
14 forget or misremember your password so that you cannot
15 withdraw cash, or you may fail to boot your computer so that
16 you cannot perform business smoothly. Because of such
17 inconvenience, the password user employs a single password
18 for multiple systems, or write down multiple passwords on his
19 notepad, for example. Such procedures compromise system
20 security that would otherwise be provided by setting up
21 passwords.

22

23 Furthermore, maintaining and using as appropriate
24 complicated passwords for each purpose would be very

1 burdensome for elderly people, and thus impractical. As the
2 society becomes more and more information-rich with a greater
3 aging population, password control and input will become a
4 significant burden for the elders.

5

6 Accordingly, it is an objective of the present invention
7 to provide an improved password generation and verification
8 system and a method therefore.

9

10 It is also an objective of the present invention to
11 provide a password generation and verification system that
12 facilitates password control and input, and a method
13 therefore.

Summary of the Invention

In order to achieve the above objectives, according to the present invention, a plurality of different categories are first selected and an element group comprised of a single or multiple password elements that belong to each category is stored in an element group storage means. When used, a specific number of categories that are randomly preset from the plurality of categories are selected. Next, a sampled password element that belongs to each of those categories is sampled from the element group storage means (if multiple password elements are provided for a single category, one of them is randomly sampled). Next, a predefined number of scramble elements that belong to the same category are randomly sampled from the scramble element storage means. The sampled scramble elements are mixed with the sampled password element, and a mixed element group, where those elements are arranged in random order, is subsequently generated on a category by category basis. The resulting mixed element group is displayed on a display means. From the group displayed, a selected password element is chosen according to the category, and correlated, on a category by category basis, by verifying means against the sampled password element stored in the password storage means. As a

1 result of the verification, if all of the selected password
2 elements match each of the sampled password elements, a match
3 signal is outputted.

4

5 The present invention that provides a method for
6 verifying a password comprises the steps of: selecting from a
7 plurality of preset categories a category to be displayed;
8 randomly selecting a sampled password element that belongs to
9 that category and a scramble element, different from the
10 sampled password element, that belongs to the same category;
11 mixing the two elements before generating, according to the
12 category, a mixed element group where they are arranged in
13 random order; displaying the element group; selecting,
14 according to the category, a selected password element from
15 the element group displayed; and verifying the selected
16 password element to the sampled password element according to
17 the same category.

Brief Description of the Drawings

Fig. 1 shows a block schematic diagram of a password generation and verification system according to the present invention;

Fig. 2 is a flowchart for explaining the procedures for generating an element group according to the present invention;

Fig. 3 is a flowchart for explaining the procedures for generating a mixed element group according to the present invention;

Fig. 4 is a diagram for explaining the concept of a password according to the present invention;

Fig. 5 is a diagram illustrating an example of how element groups are displayed on a display device;

Fig. 6 is a diagram illustrating scramble elements stored in a scramble element memory on a category by category basis;

1 Fig. 7 is a flowchart illustrating the procedures for
2 generating a password element according to the present
3 invention;

4

5 Fig. 8 is a flowchart illustrating the procedures for
6 verifying the password according to the present invention;
7 and

8

9 Fig. 9 shows a block schematic diagram illustrating one
10 embodiment that utilizes the password generation and
11 verification system according to the present invention.

Detailed Description of the Preferred Embodiment

A password generation and verification system according to the present invention offers the capabilities of generating target categories, generating a password, and verifying the password. With reference to the present invention in general, and more specifically to the capability of generating categories, a category where password elements are classified is preset by the user; the more categories, the more preferable in terms of security. They include, for example, the name of the user's acquaintance, his birthplace, alma mater (elementary school, junior high school, high school, university, etc.), name of the division to which he was first assigned in the company, name of the city where he lived in the past, name of the foreign country he visited, his habit, and so forth. They are stored in the system.

Next, with reference to the capability of generating a password, the password includes a plurality of password elements that are randomly sampled whenever it is used, and each of the password elements is preset by the user on a category by category basis. The password elements that are set are stored in the password generation and verification system.

1 Further, with reference to the capability of verifying
2 the password, the system generates a mixed element group
3 where randomly sampled scramble elements are added to a
4 sampled password element that is arbitrarily sampled
5 according to the category selected by the system (there may
6 be a password element that is singularly determined at all
7 times when a category, such as birthplace, is selected, or a
8 plurality of password elements, such as the user's
9 acquaintances; in the latter case, one of them is randomly
10 sampled by the system). The mixed element group includes the
11 sampled password element that was preset by the password user
12 and has been sampled by the system as described above, and a
13 plurality of scramble elements sampled by the system. The
14 password user chooses a selected password element that is
15 selected by the user from the mixed element group displayed
16 on a display device. One selected password element is chosen
17 from each element group, and when all the selected password
18 elements are chosen as appropriate, the system correlates the
19 sampled password element and the selected password element on
20 a category by category basis. As a result, if all of the
21 selected password elements match the sampled password
22 elements, the system decides that the person who entered the
23 password is an authorized user.

1 Typically, password elements are often represented by a
2 character string, but may be specific image information or
3 audio information. In the case of image information, for
4 example, images stored in a predetermined format are stored
5 as password elements into the system. The system may provide
6 images as scramble elements and permit password elements to
7 be selected on the display device. If image information is
8 used as password elements, images that are familiar to the
9 user are remembered for a long period of time, and thus
10 suitable for storage and control of the password. In this
11 way, various types of password elements may be used, though
12 the implementation of the present invention is described in
13 greater detail with reference to the drawings, in a case
14 where a password element is a character string.

15
16 Fig. 1 shows a password generation and verification
17 system 10 according to the present invention, which
18 comprises: a password generation and verification unit 16
19 including an element group setup portion 11, a scramble
20 element memory 12, a mixed element group generating portion
21 13, an input/output portion 14, and a comparator portion 15;
22 and a password setup input terminal 19 including a display
23 device 17 and an input device 18. The password generation and

1 verification unit 16 is coupled to the password setup input
2 terminal 19 via a wireline or wireless connection line 20.

3
4 First, how an element group is generated is described.
5 A password according to the present invention is randomly set
6 whenever it is used, and is made up of a plurality of
7 password elements that are sampled according to the category.
8 Each password element is arbitrarily preset by the password
9 user and stored in the element group setup portion 11 of the
10 system 10. The process of generating an element group is
11 described with reference to the flowchart of Fig. 2.

12
13 The system 10 makes available beforehand various
14 categories 1, 2, 3, ..., N, including, for example, name of the
15 user's acquaintance, his birthplace, alma mater (elementary
16 school, junior high school, high school, university, etc.),
17 name of the division to which he was first assigned in the
18 company, name of the city where he lived in the past, name of
19 the foreign country he visited, his habit, and so forth, and
20 the user of this system selects desired categories as many as
21 possible among them. For example, categories 1, 3, 8, 12, ...,
22 and K are selected. When the categories are selected, the
23 user enters familiar names to those categories. For example,
24 if category 1 is the names of acquaintances, which include

1 Tatsuo Maekawa, Taro Yamada, and Shiro Ono, then these names
2 are entered in password elements 11, 12, and 13. These
3 password elements 11, 12, and 13 are stored as a element
4 group 23a into the element group setup 11. By performing
5 similar procedures for categories 3, 8, 12, ..., K, password
6 elements for the respective categories are entered. It
7 should be appreciated that if category 8 is the birthplace,
8 the user's birthplace is singular; thus, a single password
9 element 81 is provided. In this way, once password elements
10 are entered for all the categories 1, 3, 8, 12, ..., K selected
11 by the user, they are stored into the element group setup 11
12 as element groups 23a, 23b, 23c, 23d, and 23e. Of these
13 password elements stored, a sampled password element is
14 randomly sampled by the mixed element group 13 according to
15 each category, as described below.

16
17 Next, the capability of verifying the password is
18 described. Fig. 3 is a flowchart for explaining the
19 procedures for generating a mixed element group in the mixed
20 element group generating portion of the system 10. As
21 described above, the element groups 23a, 23b, 23c, 23d, and
22 23e generated by the user of the system 10 have already been
23 stored in the element group setup 11. When the user provides
24 a password to the system 10 to attempt to obtain

1 authentication, the system 10 asks the user a category
2 inquiry number. The category inquiry number is a number that
3 determines on how many categories password elements are asked
4 to the user. Assuming here that "4" is given, then the
5 system 10 randomly specifies, for example, element groups
6 23a, 23b, 23c, and 23e from the element groups 23a, 23b, 23c,
7 23d, and 23e. The element groups that belong to those
8 specified categories differ whenever the user attempts to
9 gain authentication for the system 10. Once the element
10 groups are specified, the mixed element group generating
11 portion 13 randomly samples one of the password elements
12 contained in each element group, and thus extracts sampled
13 password elements 1, 2, 3, and 4.

14
15 Once the sampled password elements 1, 2, 3, and 4 are
16 sampled, a predefined number of scramble elements 31a, 31b,
17 31c, and 31d that belong to the same category as the sampled
18 password elements, as stored in the scramble element memory
19 12, are selected according to the category, and mixed with
20 the sampled password elements 1, 2, 3, and 4, respectively.
21 Once the sampled password elements 1, 2, 3, and 4 are mixed
22 with the scramble elements 31a, 31b, 31c, and 31d, they are
23 randomly rearranged, so that mixed element groups 32a, 32b,
24 32c, and 32d are generated for presentation on the display

1 device 17. The user selects as a selected password element
2 an element that is most familiar to him among the mixed
3 element groups presented on the display device 17. When the
4 selected password element for each category is entered, the
5 system 10 performs verification with the sampled password
6 element on a category by category basis. If all are matched,
7 the system 10 generates a match signal and gives
8 authentication to the user.

9
10 The above process is further described with reference to
11 the block diagram 10 shown in Fig. 1. First, setting of
12 element groups is described. Password elements are provided
13 by the password user via the input device 18. Initially, the
14 number of categories for entering the password elements is
15 inquired from the password generation and verification unit
16 16, and password elements are entered for each of the
17 categories corresponding to that number. Alternatively, a
18 list of categories made available by the system may be
19 displayed on the display device 17 to permit the user to
20 select them. Element groups may also be selected via a
21 dedicated terminal unit, which is especially needed in banks
22 and so forth where a high level of password security is
23 demanded. Password elements are set as classified on a
24 category by category basis; for example, "7" is entered as

1 the number of categories, so that the name of acquaintance,
2 birthplace, alma mater, name of division to which the user
3 was first assigned in the company, name of the city where he
4 lived in the past, name of the foreign country he visited,
5 and habit are selected as categories. For example, when
6 password elements in the name of acquaintance category are
7 set, Tatsuo Maekawa, Taro Yamada, and Shiro Ono are set as
8 the names of acquaintances. If the user lived in Hakodate,
9 Tucson, Yamagata, and Lyon, then Hakodate, Tucson, Yamagata,
10 and Lyon are entered as the names of the cities he lived in
11 the past. In this way, the names most familiar to the user
12 for each category are set, according to the category, as
13 password elements into the element group setup 11 from the
14 input device 18 via the connection line 20.

15
16 A password according to the present invention is made up
17 of multiple password elements, but each password element is
18 sampled from among the preset element groups as described
19 above. Fig. 4 conceptually depicts the structure of a
20 password 40 sampled as described above, where the password
21 elements sampled and their respective assigned category
22 numbers 41, 42, 43, and 44 are stored in pair into the
23 element group setup portion 11. The category numbers are
24 used when selecting scramble elements described below. It

1 should be noted that a combination of password elements that
2 comprise the password 40 differs whenever the user attempts
3 to gain authentication for the system 10.

4

5 Next, entering and verifying the password is described.

6 The mixed group generating portion 13 of the system 10 asks a
7 category inquiry number to the user who enters the password.

8 For example, if a category number "4" is entered from the
9 input device 18, the mixed element group generator 13

10 randomly selects four categories from the preset categories

11 of element groups. For example, the name of acquaintance,

12 birthplace, name of elementary school, and name of division

13 categories are selected, and sampled password elements are

14 randomly sampled from the password elements that have been

15 set for each category. The fixed element group generator 13

16 extracts from the scramble element memory 12 a plurality of

17 scramble elements that belong to the same category as the

18 sampled password element, and mixes them with the sampled

19 password element to generate a mixed element group where they

20 are arranged in random order. For example, the mixed group

21 generator 13 extracts a sampled password element, "Taro

22 Yamada", from the element group setup portion 11. As shown

23 in Fig. 4, the category number "1" is assigned to "Taro

24 Yamada"; thus, when the element group generator 13 recognizes

1 that "Taro Yamada" is the name of acquaintance, a
2 predetermined number of names, for example, "Shiro Saito",
3 "Hajime Ogawa", "Yoshihiko Ichikawa", "Toru Kato" are
4 randomly chosen as scramble elements from the names stored in
5 the scramble element memory 12. The scramble elements chosen
6 are missed with the password element and rearranged in random
7 order to generate a mixed element group. In this way, the
8 mixed element group generated for each category is sent to
9 the display device 16.

10
11 Figs. 5 (1)-(4) show examples of mixed element groups
12 according to the category, i.e., "name of acquaintance",
13 "birthplace", "name of elementary school", and "name of
14 division", presented on the display device 16. Referring to
15 the mixed element groups displayed on the display device 16,
16 the password user selects a certain password element and
17 enters its number from the input device 17. In the name of
18 acquaintance category, for example, the password user enters
19 number "4" as the selected password element "Taro Yamada",
20 because his pre-selected password element is "Taro Yamada".
21 Then, "Yokohama" is selected as the selected password element
22 in the birthplace category as shown in Fig. 5 (2); "Hodogaya
23 Elementary School" in the name of school category; and
24 "Supply Management Division" in the name of division

1 category. These selected password elements are sent via the
2 connection line 20 to the correlator 15, where they are
3 compared with the sampled password elements stored in the
4 element group setup portion 11, respectively. As a result of
5 the comparison, if the sampled password elements match all of
6 the selected password elements, a match/mismatch signal 21 is
7 outputted externally. This signal is sent to another unit
8 that utilizes the result of password verification.

9
10 Referring next to Fig. 6, scramble elements stored in
11 the scramble element memory 12 according to the category are
12 shown. As described above, because a predetermined number of
13 scramble elements are randomly sampled when a mixed element
14 group is generated, as many scramble elements as possible are
15 provided beforehand as potential candidates, on a category by
16 category basis. More specifically, a category number and a
17 serial number are assigned to a single scramble element,
18 which are stored in the memory 12. The category represents a
19 word having the same meaning, such as name and birthplace,
20 while the serial number denotes a continuous number used when
21 randomly selecting a scramble element. Words that belong to
22 category 1 are arranged in order of scramble elements, SE11,
23 ..., SE17, and so on; words that belong to category 2 are
24 arranged in order of scramble elements, SE21, ..., SE27, and so

1 on. For example, when a scramble element of category 1 is
2 sampled, if "5" is generated by random-number generation,
3 then scramble element, SE15, corresponding to that number is
4 chosen. A predetermined number of scramble elements chosen
5 in this way are sent to the element group generator portion
6 13. A similar process is also performed for categories 2 and
7 3.

8
9 Next, the procedures for how a password element is set
10 by the password user in the password generation and
11 verification system are described in accordance with the
12 flowchart 70 shown in Fig. 7. When the password generation
13 and verification system 10 enters the password element
14 generation mode, it firsts sets the element group inquiry
15 number and element group option number, at block 71. The
16 element group inquiry number, which is a number of categories
17 used for inquiry among a plurality of categories available,
18 is "4" in the above example, while the element group option
19 number is "5", as shown in Fig. 5. In this embodiment, the
20 element group number and element group option number are
21 queried at block 71, although the system may have their
22 default (or preset) values. Once the element group number
23 and element group option number are set, an element group
24 category(s) is selected, at block 72. The password user may

1 select desired category(s) within the range of the element
2 group number selected at block 71. For this selection, the
3 system may list prearranged categories on the display device
4 16 to allow the password user to choose from the categories
5 listed. In the above example, "name of acquaintance",
6 "birthplace", "name of elementary school" and "name of
7 division" are selected.

8
9 Once the desired categories are set, the process
10 proceeds to block 73, where a password element(s) for each
11 category is entered. For example, in the "name of
12 acquaintance" category, multiple names, in addition to "Taro
13 Yamada", are entered. At block 74, it is determined whether
14 password elements have been entered for all of the
15 categories. If not, the process returns to block 73, where a
16 similar process as described above is performed. If password
17 elements have been entered for all of the categories, the
18 process proceeds to block 75.

19
20 At block 75, the display device 16 displays all the
21 password elements by category, and if there is any password
22 element to be modified, the password user modifies the
23 password element at block 77. When all of the password
24 elements displayed are acceptable at block 76, or when

1 modification of password elements is completed at block 77,
2 the process proceeds to block 78, where the password user
3 enters the re-set password elements by category, and checks
4 if the input of the password user is accurate. When this
5 check is completed, the password generation and verification
6 unit 15 completes the password input and setup.

7
8 Next, the procedures for verifying the password are
9 described in accordance with the flowchart 80 shown in Fig.

10 8. First, when the verification system 10 is activated and
11 enters the verification mode, the element groups, as shown in
12 **Fig. 4, are displayed by category on the display device 16,**
13 at block 81. Proceeding to block 82, the password user
14 enters a desired number from the items presented on the
15 display device 16, using a keypad of the input device 17.
16 For example, in the name of acquaintance category, if it is
17 judged that "Taro Yamada" is the selected password element of
18 this category, then "4" is pressed on the keypad.
19 Alternatively, the cursor may be scrolled to select its
20 relevant position. Once the selected password element is
21 entered, that selected password element is stored in the
22 memory, at block 83. Proceeding to block 84, it is
23 determined whether all of the selected password elements have

1 been entered; if not, the process proceeds to block 81, where
2 a similar process is performed as described above.

3

4 At block 84, once all of the selected password elements
5 have been entered, the process proceeds to block 85, where
6 the pre-sampled password elements and the selected password
7 elements entered are correlated each other. If all of the
8 selected password elements match the sampled password
9 elements, a match signal is outputted at step 87; if at least
10 one of the selected password elements does not match the
11 sampled password elements, a mismatch signal is outputted.

12

13 As described above, the selected password elements
14 entered from the password input terminal 18 are compared
15 against the preset sampled password elements, and if they
16 match all of the sampled password elements, authentication
17 can be provided to the password user.

18

19 It should be appreciated that in the procedures shown in
20 Fig. 7, after all of the selected password elements have been
21 entered, verification with the pre-sampled password elements
22 is initiated; however, as each of the selected password
23 element is entered, it may be compared with the sampled
24 password elements. In that case, at a time when a

1 mismatching selected password element is entered, the
2 verification mode may be terminated to provide a notification
3 to the person who entered the selected password that a
4 password input error occurred. It should also be appreciated
5 that a mismatch signal is outputted at block 88, although
6 this process is not especially needed, but only a match
7 signal at block 87 may be outputted externally.

8
9 The password generation and verification system
10 according to the present invention may be applicable to
11 various apparatuses and systems, thereby improving the
12 security for those apparatuses and systems. Fig. 9 shows a
13 block schematic diagram where a password generation and
14 verification system 93 according to the present invention is
15 applied to a computer system 92 installed in a bank 91. The
16 computer system 92, which processes banking transactions, is
17 typically coupled to a terminal equipment 95 installed at a
18 remote site via a wireline or wireless line 94, including
19 private or public lines. The terminal equipment 95 is often
20 an automatic teller machine (ATM), but may also be a home
21 computer terminal connected to a fixed or cellular telephone,
22 due to recent proliferation of the Internet or i-mode service
23 offered by NTT of Japan. When an access is made from the
24 terminal equipment 95 to the computer system 92, the password

1 generation and verification system 93 correlates to determine
2 whether the password sent from the terminal equipment 95
3 matches the preset password. According to the present
4 invention, it is determined whether the all of the selected
5 password elements sent from the terminal equipment 95 match
6 the password elements stored in the computer system 92. If
7 all match, the computer system 92 provides authentication to
8 the person who operates the terminal equipment 95 as an
9 authorized person. This authentication allows the terminal
10 equipment 95 to be coupled to the computer system 92, so that
11 various transactions may be instructed.

12
13 In the above embodiment, the present invention is
14 applied to improve the security for the computer system in
15 the bank, although it may also be applicable to any computer
16 system of public organizations that requires authentication
17 of whether a persona who operates the terminal equipment is
18 authorized or not.

19
20 In cases where a remote access is made to a corporate or
21 home computer via a wireline or wireless line, the present
22 invention may also be applied to improve system security.
23 Especially, a connection may be established with a corporate
24 or home computer from a remote office or hotel room during a

1 business trip, so that necessary information may be sent
2 and/or received at relatively low cost.

3
4 Furthermore, for management of limited-access areas,
5 such as, for example, houses, vaults, factory plants,
6 research laboratories, and military facilities, the present
7 invention may also be applied to computers that control
8 locking and unlocking of their gateways.

9
10 Only authorized persons may sometimes be allowed to
11 operate specific vehicles, machines, and apparatuses
12 (including automobiles, construction machineries, farming
13 machineries, and factory machineries). In such cases, the
14 present invention may be employed as an activation key to
15 such machineries to verify the identity of such persons.

16
17 In summary, the present invention may be basically
18 employed in circumstances where password-based identification
19 is required. In particular, a plurality of password elements
20 are used and each password element may be selected based on
21 familiar numerals and words, or image and audio information;
22 thus, unlike prior art methods, the present invention
23 eliminates the need for bothering to remember unfamiliar
24 passwords at all times.

1 On the other hand, sampling of categories and sampling
2 of correct password elements and, additionally, scramble
3 elements are performed at random by the system (although some
4 of the password elements, such as, for example, "birthplace",
5 are singularly determined at a time when a category is
6 established). This results in a very high level of
7 randomness and thus very low predictability. In other words,
8 the resulting password is very dynamic, as compared to
9 typical static passwords that are fixed for a certain period
10 of time. Accordingly, by employing a method whereby a certain
11 limitation is imposed on response time and verification is
12 denied if there is no input beyond that limitation, even if
13 the whole preset categories and password elements were leaked
14 to any third party, it would be extremely difficult for that
15 third party to provide correct answers as quickly as the
16 authorized person himself, and thus a high level of security
17 is ensured.

18
19 What is claimed is: